

REMARKS

Claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46 are pending in the application. Claim 17 has been amended to correct a dependency from canceled claim 1 to claim 45. Reconsideration of this application is respectfully requested.

With reference to Figs. 1 and 15 of the present application, the present invention concerns the configuring of a connectivity unit (CB 11A or CB 11B or CB 11) for communication with a service entity, namely, a communications service system (CSS) 20. With reference to pages 37-52, the configuring process pre-installs a set of parameters 190 (configuration parameters) in CB 11. Parameters 190 (pages 40-43) include a public-key/private-key pair and a CB Serial Number Certificate that is issued by CSS 20 acting as a certificate authority. The CB Serial Number Certificate links the public key to the identity of CB 11, e.g., the unique serial number of the CB.

With reference to page 38, once the CB unit is purchased, user information is provided by either the user or the vendor to a call center 146. The user information includes the serial number of CB 11, the user address, billing information and telephone number for the line to which CB 11 will be connected. A CB name is determined and a CB ID is generated or derived from the user information. Call center 146 then stores a record of the user information in databases 24 and 204 that are accessible by CSS 20. The stored record includes the CB ID and the CB name.

With reference to pages 45 and 46, a connection is established between CB 11 and CSS 20 using the configuration parameters 190 with the CB Serial No. Certificate being used to authenticate CB 11 to CSS 20. CSS 20 then transfers (downloads) to CB 11 a set of parameters 191 that includes a CB Certificate (user-id certificate) linking the CB public key with an identifier (e.g., the CB ID) of the user derived from user-information.

The configuration process uses two certificates. The first certificate (CB Serial Number Certificate) is pre-installed in CB 11 and links the CB identity to a public-key of a public-key/private-key pair that is also pre-installed in CB 11. This certificate is issued by CSS 20. Because it is issued by CSS 20 and because it is linked to the public key of CB 11, CSS 20 can be assured that the connected CB is truly CB 11 when CB 11 connects to CSS 20 for the configuring process.

The second certificate (CB Certificate) is transferred to CB 11 during the configuration process and links the public key of CB 11 with an identity of the user. The second certificate is subsequently used to authenticate CB 11 to CSS 20.

The second certificate is advantageous. The second certificate includes the identity of the user, which can be used by CSS 20 in one memory access to directly access the user record in databases 24 or 204. On the other hand, if the first certificate were used in subsequent communications between CB 11 and CSS 20, CSS 20 would need two memory accesses. In the first access, the CB 11 serial number would be used to access the registration record for CB 11. In the second access, the user identity contained in the registration record would then be used to directly access the user record. The savings in memory accesses provides a time and throughput efficiency.

Another advantage is that the second certificate provides an identification of the user when the user communicates with other parties. A further advantage is that the user-id certificate can be used to link together activities of the user when using different connectivity boxes.

The Office Action rejects claims 2, 31, 38, 40, 45 and 46 under 35 U.S.C 103(a) as unpatentable over International Publication No. WO 99/21336 to Slaby et al., hereafter Slaby, in view of U.S Patent No. 6,073,172 to Frailong et al., hereafter Frailong.

This rejection is erroneous for the reasons discussed in the arguments set forth below and should be withdrawn.

Argument 1.

The Slaby/Frailong combination lacks authentication using the identity-sequence certificate as recited in claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46.

Slaby pre-installs only a serial number of the unit (router). Slaby does not pre-install a public-key/private-key pair and an identity-sequence certificate linking the public key to the identity sequence of the unit, and, therefore, lacks these elements, which are recited in the pre-installing step of claims 45 and 46.

Slaby does not disclose or teach any certificates issued by a certificate authority. A certificate is known in the art as a document that is issued by a certificate authority.

Slaby uses a unit (router) serial number that during configuration is communicated to a configuration service. The Examiner contends in paragraph 25 of the Office Action that the unit is authenticated to the configuration service, citing page 9, lines 3-13. This citation merely states that the configuration service uses the serial number of the unit to access configuration data for that serial number and download the configuration data to the unit. There is no authentication that the unit sending the serial number is, in fact, the unit to which the serial number is assigned. Slaby at page 11, lines 17-20, describes that when the configuration service receives the serial number, it uses a verification process to determine whether it is a valid serial number. Verification is not authentication. Authentication involves a proof that the connected unit is indeed the unit with the communicated serial number. All that Slaby's communication service is doing is determining if the serial number is valid. If valid, the communication service still does not know if the unit that communicated the serial number is indeed the unit to which the serial number is assigned. Thus, Slaby does not disclose or teach and, therefore, lacks authentication of the unit as well as using an identity-sequence certificate for authentication, as recited in independent claims 31, 38, 45 and 46.

The Examiner contends page 3 (paragraph 4) that as for use of certificates linking a public key to an identity sequence and user id, Slaby discloses a means of security through encryption, citing page 11, lines 11-20. Encryption protects against an eavesdropper reading and understanding a message. Encryption merely encodes a message and has nothing to do with authentication. Thus, this passage contains no disclosure, teaching or suggestion of authentication.

As noted in the discussion above, using an identity sequence certificate that links the identity-sequence to a public key of a public-key/private-key pair provides an assurance that the identity sequence is indeed that of the unit to which it is assigned because (1) the certificate was initially issued by the communication service and (2) the certificate is linked to the public key. Slaby does not disclose, teach or suggest a public-key/private-key pair or a certificate that is linked to the public key. Therefore, for this additional reason, Slaby does not disclose or teach authenticating the unit to the communication service, as recited in independent claims 31, 38, 45 and 46.

Frailong does not disclose, teach or suggest authentication of a unit to a configuration service during configuration.

Frailong discloses a system in which a public key certificate is installed in a network interface by a manufacturer. Frailong does not disclose, teach or suggest configuring the network interface with any configuration entity or service.

Frailong discloses at column 18, lines 46-49 that the system supports "a variety of public key certificates incorporating different cryptographic algorithms for reasons of enhanced security and internationalization". Frailong teaches an encryption system that uses his certificates. Frailong does not disclose, teach or suggest a configuration system using his certificates in a configuration system, a connectivity unit or a configuration process for authenticating the unit to a configuration service or entity. As discussed above, Slaby does not disclose or teach authentication during configuration. Therefore, Slaby/Frailong, using a Frailong public key/private key pair, lacks authentication of the

unit to the service during a configuration procedure as recited in independent claims 31, 38, 45 and 46 and their respective dependent claims.

Argument 2.

The Slaby/Frailong combination lacks the user-identity certificate recited in claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46.

Slaby does not transfer from the service to the unit "a user-id certificate associating the public key of the unit with a user identity derived from the user related information", as recited in independent claims 31, 38, 45 and 46. The Examiner contends in paragraphs 4 and 25 of the Office Action that Slaby transfers a user-id associated with a user identity derived from the user related information, citing page 12, lines 10-13. This contention is traversed. This citation refers to the service loading a user name and password into the unit. Slaby does not disclose that either the user name or the password is derived from the user information as recited in claims 45 and 46.

Moreover, neither the user name nor the password is a certificate. As discussed in Argument 1, Slaby does not disclose or teach any certificates issued by a certificate authority. A certificate is known in the art as a document that is issued by a certificate authority.

Frailong discloses at column 19, lines 29-32, a Public Key Certificate that is installed by the manufacturer and that includes the serial number of the unit as a part of the identity. Frailong does not disclose, teach or suggest a user-id certificate that associates the public key with a user identity derived from user-related information.

The Examiner contends that the use of Frailong's certificates to identify a user, using their user id to service providers is well known in the art. This contention is challenged. The Examiner cites no evidence in support of this contention. The Examiner must cite evidence in support of this contention. In the absence of such evidence, the

contention has no probative value. Therefore, Slaby/Frailong does not have a user-id certificate as recited in independent claims 31, 38, 45 and 46.

Moreover, Frailong does not even disclose, teach or suggest modifying his certificate for association with a user or for use with a configuration service. Frailong does not even mention a configuration service.

For the above reasons, Slaby/Frailong lacks a user-id certificate as recited in as recited in independent claims 31, 38, 45 and 46 and their respective dependent claims.

Argument 3

Slaby/Frailong lacks both an identity-sequence certificate and a user-id certificate where both certificates being linked to the same public key, as recited in claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46.

Since Slaby/Frailong lacks a user-id certificate as discussed above in Argument 1, Slaby/Frailong also lacks the combination of both an identity-sequence certificate and a user-id certificate.

Moreover, neither Slaby nor Frailong discloses, teaches or suggests a need for a user-id certificate, particularly one that is linked to the same public key as the identity-sequence certificate.

For the above reasons, Slaby/Frailong lacks both an identity-sequence certificate and a user-id certificate that are both linked to the same public key, as recited in as recited in independent claims 31, 38, 45 and 46 and their respective dependent claims.

Argument 4.

Slaby/Frailong lacks using a user-id certificate for authentication during subsequent communications with the configuration service as recited in claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46.

Since Slaby/Frailong lacks a-user-id certificate as discussed in Argument 2 above, Slaby/Frailong also does not use a user-id certificate in subsequent communications to authenticate the unit to the service entity. Therefore, Slaby/Frailong lacks authentication of the unit to the configuration service with the user-id certificate being used to authenticate the unit to the service, as recited in independent claims 31, 38, 45 and 46 and their respective dependent claims.

Argument 5.

The combination of Slaby and Frailong lacks motivation.

The Examiner contends at page 4 (paragraph 4) that the combination of Slaby and Frailong is obvious because "it would have provided a means of increased security through the use of trusted certificates for authenticating users/units and further would have allowed for establishing secure communications between peers using well known standards such as Secure Socket layer".

There is no motivation for one of ordinary skill in the art to use either Slaby's unit serial number or Frailong's public key/private key certificates to authenticate a unit to a configuration service or entity. The only teaching for authentication is in Applicants' application. The use of Applicants' teaching constitutes hindsight.

Moreover, there is no motivation to combine Slaby and Frailong just because of a desire to use the Secure Sockets Layer protocol. It would seem that either Slaby or Frailong alone could use the Secure Sockets Layer protocol. The Examiner has not cited any special consideration for combining Slaby with Frailong to use the Secure Sockets Layer protocol.

The Office Action suggestion to use Frailong in combination with Slaby is improperly based on the hindsight of Applicants' disclosure. Such hindsight reconstruction of the art cannot be the basis of a rejection under 35 U.S.C. 103. The prior

art itself must suggest that modification or provide the reason or motivation for making such modification. In re Laskowski, 871 F.2d 115, 117, 10 USPQ 2d 1397, 1398-1399 (CAFC, 1989). "The invention must be viewed not after the blueprint has been drawn by the inventor, but as it would have been perceived in the state of the art that existed at the time the invention was made." Sensonics Inc. v. Aerosonic Corp. 38 USPQ 2d 1551, 1554 (CAFC, 1996), citing Interconnect Planning Corp. v. Feil, 774 F. 2d 1132, 1138, 227 USPQ 543, 547 (CAFC, 1985).

For the reasons set forth above, the combination of Slaby and Frailong lacks motivation.

For the reasons set forth above in Arguments 1, 2, 3, 4 and 5, it is submitted that the rejection of claims 2, 31, 38, 40, 45 and 46 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 10, 33 and 39 under 35 U.S.C 103(a) as unpatentable over Slaby in view of Frailong and further in view of U.S Patent No. 6,105,131 to Carroll, hereafter Carroll.

This rejection is erroneous for the same reasons set forth in the discussion of the rejection of independent claims 45, 31 and 38 from which claims 10, 33 and 39 depend.

For the reason set forth above, it is submitted that the rejection of claims 10, 33 and 39 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 11-13, 17-19, 35, 41 and 42 under 35 U.S.C 103(a) as unpatentable over Slaby in view of Frailong and further in view of an article entitled "Remote Authentication Dial In User Service (RADIUS), by Rigney et al., hereafter Rigney.

This rejection is erroneous for the same reasons set forth in the discussion of the rejection of independent claims 45, 31 and 38 from which claims 11-13, 17-19, 35, 41 and 42 depend.

For the reason set forth above, it is submitted that the rejection of claims 11-13, 17-19, 35, 41 and 42 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

The Office Action rejects claims 21, 23, 36 and 37 under 35 U.S.C. 103(a) as unpatentable over Slaby in view of Frailong and further in view of U.S. Patent No. 6,526,131 to Zimmerman et al., hereafter Zimmerman.

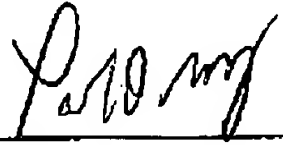
This rejection is erroneous for the same reasons set forth in the discussion of the rejection of independent claims 45 and 31 from which claims 21, 23, 36 and 37 depend.

For the reason set forth above, it is submitted that the rejection of claims 21, 23, 36 and 37 under 35 U.S.C. 103(a) is erroneous and should be withdrawn.

It is respectfully requested for the reasons set forth above that the rejection under 35 U.S.C. 103(a) be withdrawn, that claims 2, 10-13, 17-19, 21, 23, 31, 33, 35-42, 45 and 46 be allowed and that this application be passed to issue. In the event it is deemed that this Amendment does not place the application in condition for allowance, it is respectfully requested that the Amendment be entered for the purpose of Appeal.

Respectfully Submitted,

Date: 4-6-05



Paul D. Greeley
Reg. No. 31,019
Attorney for Applicants
Ohlandt, Greeley, Ruggiero & Perle, L.L.P.
One Landmark Square, 10th Floor
Stamford, CT 06901-2682
(203) 327-4500